# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-132173
(43)Date of publication of application : 09.05.2003

(51)Int.Cl. G06F 17/60

(21)Application number : 2002-246418 (71)Applicant : HEWLETT PACKARD CO <HP>
(22)Date of filing : 27.08.2002 (72)Inventor : ERICKSON JOHN S
SCHLAGETER MARK

(30)Priority
Priority number : 2001 941606 Priority date : 30.08.2001 Priority country : US

(54) ELECTRONIC MEDIA CONTAINER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method capable of storing and transferring the media contents and processing the media contents without limiting the number of kinds of media while keeping the security to the copyright infringement conduct.
SOLUTION: A single 'container' for storing and/or transferring the electronic data is provided. The container includes the data used in designating the format of the capsulized data to various applications of a wide rangereferring the right management technology used in packaging the dataand further providing the policy relating to a method of acquiring and interpreting the data contents.

CLAIMS

[Claim(s)]
[Claim 1]Are a secure electronic-media container which saves right management Interface Division to electronic-media contentsand transmits itand/or is providedand said containerSaid electronic-media contents stored in itand data which is added to the exterior of this container or is related with this containerA secure electronic-media container provided with a typical media hair drier and a right management

mechanism required in order to open said contents and to reproduce.

## DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]Especially this invention relates to the software media container format for storing electronic content safely about a software media container. This container is suitable for especially using it with the management application of the digital rights in connection with execution of an electronic policyor the mechanism of copyright protection.

[0002]

[Description of the Prior Art]Copyright is intellectual property rights granted to the creator of a specific kind of workand the creator can manage various directions of the work according to copyright. Copyright is for protecting publication of literaturetheatermusicthe original article of fine artsand a worksound recordinga movie (video is included)and broadcast (cable broadcasting and satellite broadcasting are included).

The right provided by copyright reaches various fieldssuch as a duplicate of such a work protectedadaptationsdistribution of a reproductionpublic demonstrationand broadcast.

In many casesan author has the right to display a name on its own workand the right to make an objection to excision and modification of its own work. Since the lending rights of sound recordinga movieand a computer program are granted to the owner of copyrightit is necessary to acquire a license from an owner of a copyright to use it by lending such a work to the public.

[0003]In recent yearsit is becoming increasingly general to save electronically contentssuch as sound recordinga literary workand a movieand a commercial sale of such electronic content by retail storessuch as a record shop and a bookstoreis made from the former. Although there are many advantages in commercial sale of the electronic content through an information technology networkCommercial sale of electronic content is not necessarily widely adopted as the creator or vendor of contents by making into the main Reasons concern of a third party reproducing and selling and becoming easy to distribute such contents unlawfully as a result. For this reasongreat efforts have been paid towards development of the technical measure which prevents the unjust duplicate of electronic content.

[0004]An illegal duplicate is comparatively easy for digital contents. For the donor of contentsthis is desirablein order to distribute contents as widely as possible (value by it). [ increase and ] Thereforeit is also inconvenient at the point that it is desirable to pay a price at every sale certainly in that the potential income obtained from there

becomes large while it is convenienti.e.piracy (copyright infringement) is not performed. In order to prevent the above piracythe donor of contents tends to adopt a digital protection system (usually based on encoding technology)but. These have the problem that it may be weakened by the free and illegal system which provides an easy user with the contents same in c where expense starts b management with difficult restriction of distribution that it is hard to use to a consumer.
[0005]One of the known protection systems is provided from Microsoft Digital Media System. In this systemelectronic content is provided with a key. The corresponding key obtained from a regular keyserver is required of a userand he can reproduce contents after that. One of the main faults of this system is that the connection with a user's playback equipment is strong at the point that equipment for exclusive use is needed in wishing reproduction of the contents protected by this system.
[0006]Generallymany of managing systems of known digital rights and protection systems are substantially accompanied by encryption of the work.
The duplicate and/or reproduction of contents which were reproduced by this are difficult.
The digital-rights-management (DRM:Digital rights management) technology used now is known by the user also as a secure container. That isa secure container defines an original file format and encapsulates arbitrary media files safely in it.
[0007]For exampleUS6138119B is indicating the technology for definingusing and operating a right management data structureand has realized safe and positive preservation and transmission of digital contents using the concept of a secure digital container. Since an alteration is difficult for such a containerit can use in order topackage-ize digital information of arbitrary kindssuch as a textgraphicssoftware that can be performedan audioor videofor example. Howeverby this methodthe situation where the contents made into safety (secure) can be used is limited.
[0008]A system another type provides "plug-in" security function to specific media formats (Adobe(trademark) PDF etc.). A software plug-in business modelVideoan audio (connectable codec)multimedia (connectable execution program "extends" a program)Although the Creativity tool (filter which extends the Image Processing Division tool)a web browseretc. have been used for extension of application over many years in other specific commercial scenesonly Adobe Acrobat (trademark) provides the security function now.
A third party's developer can develop uniformly DRM which functions in a specific format using this security function.
Howeverthe technique used by this system is restricted by the media function of a target format (PDF). That isthis technique restricts the number of the kinds of media which can carry out safing to a single format.
[0009]
[Problem to be solved by the invention]One of the main problems in the field of digital rights management (DRM) is a problem of compatibility (interoperability). That isit is

the solution which can provide arbitrary media content with the format which can apply various arbitrary DRM policies if needed. If it puts in another waypreservation and transmission of media content are possibleand the method which restriction twists is needed for the number of the kinds of media which can be processedmaintaining the security to piracy. This invention tends to cope with this problem and tends to solve the above-mentioned problem.
[0010]
[Means for solving problem]According to the 1st mode of this inventionthe secure electronic-media container which saves right management Interface Division to electronic-media contentsand transmits itand/or is provided is provided. This container is provided with the following.
Electronic-media contents stored in it.
Data which is added to the exterior of a container or is associated by other methods. A typical media hair drier.
And/ora right management mechanism required in order to open contents and to reproduce.

[0011]According to the 2nd mode of this inventionthe equipment which processes the contents of the secure container defined by the 1st mode of this invention is providedand the electronic-media contents of arbitrary formats are stored in this secure container. A means for this equipment to determine from external data what the right management mechanism used for package-ization of contents will be (if it is)and to take out a suitable digital-rights-management hair drieror to access itA means to pass contents via a DRM hair drierand a means to determine a media hair drier required for access and processing to contents from external dataand to take out a suitable media hair drieror to access itIt has a means to pass contents via a media hair drier.
[0012]According to the 2nd mode of this inventionthe method of processing the secure container defined by the 1st mode of this invention is also providedand the electronic-media contents of arbitrary formats are stored in this secure container. It is determined as this method what the right management mechanism which read external data and was used for package-ization of contents will be (if it is)The step which takes out a suitable digital-rights-management hair drieror accesses itThe step which passes contents via a DRM hair drierand the step which reads external data and determines a media hair drier required for access and processing to contentsThe step which takes out a suitable media hair drier or accesses itand the step which passes contents via a media hair drier are contained.
[0013]The concept of a secure container is well-known in a field for the time beingand it defines as this Description widely from a viewpoint of the abstract data container format for storing data. Inside a container provided with notional packagei.e.a "trumpet"which surround and protect the stored dataData can use it for

datareconstructingonly when the specific software program which is encipheredor is adjusted with other methods and adjusted especially for the format is used. Other than being based on the above-mentioned specific software programin the exterior of a containerdata cannot be accessed at the information relevant to iteitherandin the case of the secure container by conventional technologyit cannot reconstructeither.
[0014]On the other handthis invention provides a secure container with the form of universal "envelope" in consideration of arbitrary media formats and arbitrary DRM mechanismsi.e.a meta-container. or [ that this adds metadata to the secure container containing media content ] -- or it realizes by connecting. Generallysince the media format (underlying) and digital-rights-management mechanism of the bottom which can read metadata universallyand/or can decode it and are used for "package-ization" of contents are describedApplication of the copyright management policy by which processing applications (for examplea desk-top software toola web browseretc.) were displayed and specified as evaluation of the processing condition of a containerextraction (if required) of the component to processand extraction of owner-of-a-copyright information is attained.
[0015]Can standardize the format (it can be regarded as a package or "trumpet" itself) of the "outer layer" of a media containerand this formatSince the mechanism which can create "plug-in" solution based on the proposal of the value that various DRM vendors differ is providedcompatibility is easily realizable using the concept of this invention. These DRM plug-in is constituted so that an original protocol may be applied if neededrespectivelyand even if what kind of DRM user interfacekey managementtransaction messagingetc. are requiredit can send it out. These appear as expansion to the target media display application.
[0016]
[Mode for carrying out the invention]A situation of transmitting the secure container 12 containing electronic contentsuch as sound recordingto the user 10 with reference to drawing 1 is considered. Since data is stored in the secure container 12software special to reconstructing sound recording and reproducing is needed. The common container hair drier 15 takes out details of a DRM mechanism used in order to package-ize data in the secure container 12and details of a media hair drier required in order to process data (if it is). These details are attached to an outer layer of the container 12 as metadata with details about how and where or a required media hair drier and a DRM hair drier are acquirable (if they are suitable). Contents can be passed via the DRM hair drier 14 specified firstit can be passed via a media hair drier specified as the nextandas a resultthe user can reproduce sound recordingand a suitable DRM policy can be applied.
[0017](It is contained in metadata) The standard of a DRM formatHow to take [ recognizes and refers to the media hair drier 16 which the common container (or envelope) hair drier 15 needsand/or ] out (if necessary) is expressedand the method for recognizing and referring to a specific DRM hair drier or plug-in especially is

expressed. A DRM mechanism can be referred to in a way similar with the MIME type being processed now.
[0018]How a container hair drier and/or a media hair drier communicate with each host application is generated on various levelsand since it is well-known in a field for the time beingit does not explain to details any more here. If a DRM format hair drier opens the file as which the DRM mechanism is specifieda DRM format hair drier will call specified plug-in or remote serviceand will process it. Howeverthis Description is not related but a correspondence procedure with the contents which this plug-in or service performsand a userand the correspondence procedure on a network change it by a program. The advantage that arbitrary media formatssuch as WordMP3PDFand HTMLcan be chosen as a "markup"and it can package-ize by this using arbitrary security solutions is acquired. If it puts in another wayit can be considered that this invention provides the DRM compatibility of a format level. Although the party concerned seems to use the same media format by thisthe secure container which has actually the trumpet (wrapper) of the format defined by this invention is used.
[0019]Nextwith reference to drawing 2the illustration markup format according to this invention is explained in detail.
[0020]Generally structure markup syntaxsuch as XMLis being used for the container according to the illustration embodiment of this inventionand it is provided with the <CONTENT> section and the <DRM> section at least.
[0021]The <CONTENT> section specifies the format (for exampleMIME type) of contents. this section -- contents -- encapsulating (many are as "BUROBBU (blob)" of a hexadecimal code) -- or it is preferred that it can specify indirectly with the address (for exampleURL or DOI) of a network resource. The reference (option) to the Web location of a descriptive metadata and format standard and the reference (option) to the location of "rendering" code registry are included in other elements in the <CONTENT> section.
[0022]The <DRM> section specifies the DRM mechanism (typically encryption mechanism only for media) used for package-ization of contents. The specified mechanism is included into the <CONTENT> sectionor is referred to with the <CONTENT> section. The reference destination of DRM is the component installed in the local systema remote componentor web service. Therefore. [ whether local contents BUROBBU should be transmitted to remote DRM web service by DRM format for processingand ] It can be specified whether the enciphered remote contents stream should be thawed by remote web serviceor a remote source stream should be processed with a local resource.
[0023]The processing order of the element (a file or a stream) in the <DRM> container is an order that the <CONTENT> element always continues after the <DRM> element. Thereforewhen it judges that call application opens an outside DRM envelope and the DRM mechanism is specifiedthis applicationIt recognizes that contents must be passed via the DRM mechanism (it is (like a filter)) specified firstthe

suitable media hair drier for the next must be calledand a contents type must be processed by the given definition of a DRM format. By such a processing modeladvanced applicationssuch as a multistep DRM mechanismbecome possibleand contents are passed by a series of specified DRM mechanisms.
[0024]The suitable processing of the media type of an object needs to be cautious of it being dependent on application. For examplewhen [ specific ] a hair drier has a role which performs "code conversion" of an HTML file using the embedded <DRM> objectthe right "processing" methodIt is inserting in an output stream the suitable HTML tag set by the MIME type with which contents were specified.
[0025]In one mounting consideredthe DRM mechanism can place the metadata structure (for exampleXML file) "was extracted" from contents via processing of itself under the authority of another department. This can be strengthened by a media hair drier (for examplepeculiar right metadata already embedded). Regardless of itthe standard formatted by XML (for example) of the way a DRM mechanism "describes" that the call of proxy server equipment (app) should process contents is (rather) received. Thereforethe DRM mechanism can pass a "proposal" to app about the method of controlling a menu item etc. The role of app actually performs it. Control metadata is package-ized so that the standard of a ("filter" concept) and a lot may be eventually passed to appwhen using two or more mechanisms.
[0026]If it summarizesthis invention provides single "container" which saves and/or transmits electronic data. The format of the encapsulated data is specified as this container to wide range various applicationsThe data which can be used in order to provide the policy about the method of acquiring and interpreting data contents furtherwith reference to the right management technology used for package-ization of data is contained (to exterior of a "container").
[0027]Following embodiments are contained in this invention as an example.
[0028]1. Are a secure electronic-media container (12) which saves right management Interface Division to electronic-media contentsand transmits itand/or is providedand said containerSaid electronic-media contents stored in itand the data which is added to the exterior of this container (12)or is related with this containerA secure electronic-media container provided with a typical media hair drier (16) and a right management mechanism required in order to open said contents and to reproduce.
[0029]2. If it is equipment with which the electronic-media contents of arbitrary formats are stored and which processes the contents of the secure container (12) of a description to the above 1 and isIt is determined from the data of the aforementioned exterior what the digital-rights-management mechanism (14) used for package-ization of said contents is(15) means to take out a suitable digital-rights-management hair drier (14)or to access itA means to pass said contents via said digital-rights-management hair drier (14)Equipment provided with a means to determine a media hair drier (16) required for access and processing to contents from the data of the aforementioned exteriorand to take out a suitable media hair drieror to

access itand a means to pass said contents via said media hair drier (16).
[0030]3. The media content which the metadata which describes the media format (underlying) and digital-rights-management mechanism of the bottom which could read universallyand/or could decode and was used for package-ization of contents is attachedor is combined. A secure electronic-media container (12) given in the above 1 containing the secure container which it has.
[0031]4. Secure electronic-media container given in the above 3 in which said metadata describes media format of the bottom which encapsulates contents themselves.
[0032]5. Secure electronic-media container given in the above 3 in which said metadata describes media format of the bottom including remote network resource address where contents themselves are saved.
[0033]6. Secure electronic-media container given in the above 3 containing descriptive metadata or more relevant to any one of reference to resource location of said contents and format standardand the references to location of "rendering" code registry in said metadata.
[0034]7. Said metadata which describes the digital-rights-management mechanism used for package-ization of contentsA secure electronic-media container given in the above 3 which can refer to the componentremote componentor network service installed on the local system.
[0035]8. It is the method of processing the contents of the secure container (12) of a description to the above 1 in which the electronic-media contents of arbitrary formats are storedIt is determined what the digital-rights-management mechanism (14) used for package-ization of said contents if the data of the aforementioned exterior was read and it was isThe step which takes out a suitable digital-rights-management hair drier (14)or accesses itThe step which passes said contents via said digital-rights-management hair drier (14)The step which reads the data of the aforementioned exterior and determines a media hair drier (16) required for access and processing to contentsEquipment provided with the step which takes out a suitable media hair drier or accesses itand the step which passes said contents via said media hair drier (16).
[0036]As mentioned abovethis invention was explained with reference to the specific illustration embodiment. Howeverprobablyit will be clear to a person skilled in the art for not deviating from the pneuma and the range of this invention for various modification and change to be possible. Thereforeit should be considered that this Description and Drawings are the examples instead of limitation.

## DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a schematic block diagram explaining the function of the illustration embodiment of this invention.

[Drawing 2]It is a figure showing the typical DRM file format according to this invention.

[Explanations of letters or numerals]

12 An electronic-media containera secure container

14 A right management mechanisma DRM hair drier

15 Container hair drier

16 Media hair drier

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－132173
（P2003－132173A）
(43)公開日　平成15年5月9日(2003.5.9)

| (51)Int.Cl.⁷ | 識別記号 | Ｆ Ｉ | ﾃｰﾏｺｰﾄﾞ(参考) |
|---|---|---|---|
| Ｇ０６Ｆ　17/60 | １４２ | Ｇ０６Ｆ　17/60 | １４２ |
| | ３０２ | | ３０２Ｅ |
| | ５１２ | | ５１２ |
| | ＺＥＣ | | ＺＥＣ |

審査請求　未請求　請求項の数1　ＯＬ　（全 7 頁）

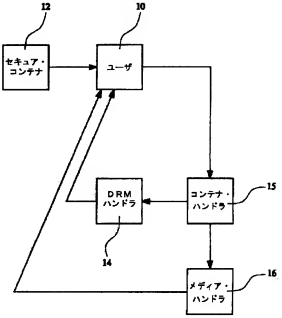
(21)出願番号　特願2002－246418(P2002－246418)
(22)出願日　平成14年８月27日(2002.8.27)
(31)優先権主張番号　０９／９４１，６０６
(32)優先日　平成13年８月30日(2001.8.30)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　398038580
ヒューレット・パッカード・カンパニー
HEWLETT－PACKARD COMPANY
アメリカ合衆国カリフォルニア州パロアルト　ハノーバー・ストリート　3000
(72)発明者　ジョン・エス・エリクソン
アメリカ合衆国05055バーモント州ノーウィッチ、ルート・132　707
(74)代理人　100081721
弁理士　岡田　次生　（外２名）

最終頁に続く

(54)【発明の名称】　電子メディア・コンテナ

(57)【要約】
【課題】　メディア・コンテンツの保存と転送が可能であり、著作権侵害行為に対するセキュリティを維持しつつ、処理できるメディアの種類の数に制限がない方法を提供する。
【解決手段】　本発明は電子データを保存及び/または転送する単一の「コンテナ」を提供する。このコンテナには、カプセル化されたデータのフォーマットを広範囲の様々なアプリケーションに対して指定し、データのパッケージ化に使用された権利管理技術を参照し、さらにデータ・コンテンツを取得し解釈する方法に関するポリシーを提供するために使用できるデータが含まれる。



【特許請求の範囲】
【請求項１】権利管理インターフェイスを電子メディア・コンテンツに保存し転送し及び/または提供するセキュア電子メディア・コンテナであって、
前記コンテナは、その中に格納される前記電子メディア・コンテンツと、該コンテナの外部に付け足されるかまたは該コンテナに関連付けられるデータと、典型的なメディア・ハンドラと、前記コンテンツを聞いて再生するために必要な権利管理メカニズムとを備えるセキュア電子メディア・コンテナ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ソフトウェア・メディア・コンテナに関し、特に電子コンテンツを安全に格納するためのソフトウェア・メディア・コンテナ・フォーマットに関する。このコンテナは、電子的なポリシーの執行や著作権保護のメカニズムに関わるデジタル権利の管理アプリケーションで使用するのに特に適している。
【０００２】
【従来の技術】著作権は特定の種類の作品の創作者に与えられる知的財産権であり、創作者は著作権によってその作品の様々な利用法を管理できる。著作権は、文学、演劇、音楽、美術の原作品、作品の出版、録音、映画（ビデオを含む）、放送（有線放送、衛星放送を含む）を保護するためのものであり、著作権によって提供される権利は、このような保護されている作品の複製、翻案、複製物の配布、公共における実演、放送などの様々な領域に及ぶ。また、多くの場合、著作者は、自分の作品に氏名を表示する権利と、自分の作品の切除や変形に異議を唱える権利を有する。さらに、著作権の所有者には録音物、映画及びコンピュータ・プログラムの貸与権が与えられるので、このような作品を公衆に貸与することによって使用するには著作権者からライセンスを得る必要がある。
【０００３】近年、録音物、文学作品及び映画などのコンテンツを電子的に保存することがますます一般的になってきており、またレコード店や書店などの小売店によるこのような電子コンテンツの商業的販売は従来から行われている。情報技術ネットワークを介した電子コンテンツの商業的販売には多くの利点があるが、結果としてこのようなコンテンツをサード・パーティーが不法に複製、販売、配布しやすくなるのではないかという懸念を主な理由として、電子コンテンツの商業的販売はコンテンツの創作者や販売業者に広く採用されているわけではない。このため、電子コンテンツの不正な複製を防止する技術的な対策の開発に向けて多大な努力が払われてきた。
【０００４】デジタル・コンテンツは不法な複製が比較的容易である。このことは、コンテンツの提供者にとって、コンテンツをできるだけ広く配布するためには望ましい（それによって価値が高まり、従ってそこから得られる潜在的な収入も大きくなる）という点で好都合である一方、販売のたびに確実に代金が支払われること、つまり海賊行為（著作権侵害）が行われないことが望ましいという点で不都合でもある。前述のような海賊行為を防止するために、コンテンツの提供者はデジタル保護方式（通常は暗号化技術に基づく）を採用する傾向があるが、これらは、ａ）消費者には使いにくく配布の制限が難しい、ｂ）管理に費用がかかる、ｃ）同一のコンテンツを安直なユーザーに提供する無料かつ不法な方式によって骨抜きにされる可能性があるという問題がある。
【０００５】既知の保護方式の１つは、Ｍｉｃｒｏｓｏｆｔ Ｄｉｇｉｔａｌ Ｍｅｄｉａ Ｓｙｓｔｅｍから提供されている。この方式では、電子コンテンツはキーと共に提供される。ユーザーは、正規のキー・サーバーから得られる対応するキーを要求され、その後コンテンツを再生することができる。この方式の主な欠点の１つは、この方式で保護されたコンテンツの再生を希望する場合には専用の装置が必要になるという点で、ユーザーの再生装置との結び付きが強いことである。
【０００６】一般に、既知のデジタル権利の管理方式及び保護方式の多くは、実質的に作品の暗号化を伴っており、これによって複製されたコンテンツの複製及び/または再生が困難になっている。現在使用されているデジタル権利管理（ＤＲＭ：Ｄｉｇｉｔａｌ ｒｉｇｈｔｓ ｍａｎａｇｅｍｅｎｔ）技術は、ユーザーには、セキュア・コンテナとしても知られている。すなわち、セキュア・コンテナは独自のファイル・フォーマットを定義し、その中で任意のメディア・ファイルを安全にカプセル化する。
【０００７】例えば、米国特許第６１３８１１９号は、権利管理データ構造を定義し、使用し、操作するための技術を開示しており、セキュア・デジタル・コンテナの概念を使用してデジタル・コンテンツの安全かつ確実な保存と転送を実現している。このようなコンテナは改ざんが難しいので、例えば、テキスト、グラフィック、実行可能ソフトウェア、オーディオまたはビデオ等の任意の種類のデジタル情報をパッケージ化するために利用することができる。しかし、この方法では安全（セキュア）にされたコンテンツを利用できる状況が限定される。
【０００８】別のタイプのシステムは、特定のメディア・フォーマット（Ａｄｏｂｅ（商標）ＰＤＦなど）に対して「プラグイン」セキュリティ機能を提供する。ソフトウェア・プラグイン・ビジネスモデルは、ビデオやオーディオ（接続可能なｃｏｄｅｃ）、マルチメディア（プログラムを「拡張」する接続可能な実行プログラム）、クリエイティビティ・ツール（画像処理ツールを拡張するフィルタ）及びＷｅｂブラウザなど、他の特定の市場では長年にわたってアプリケーションの拡張に使

用されてきたが、現在ではＡｄｏｂｅ　Ａｃｒｏｂａｔ（商標）のみがセキュリティ機能を提供しており、サード・パーティーのディベロッパーはこのセキュリティ機能を用いて特定のフォーマットで機能するＤＲＭを一律に開発することができる。しかし、このシステムで用いられる手法は、ターゲット・フォーマット（ＰＤＦ）のメディア機能によって制限される。つまり、この手法は、単一のフォーマットに対して、安全化することができるメディアの種類の数を制限する。

【０００９】

【発明が解決しようとする課題】デジタル権利管理（ＤＲＭ）の分野における主な問題の１つは、相互運用性（interoperability）の問題である。すなわち、必要に応じて様々な任意のＤＲＭポリシーを適用できるフォーマットを任意のメディア・コンテンツに提供することができる解決法である。換言すれば、メディア・コンテンツの保存と転送が可能であり、海賊行為に対するセキュリティを維持しつつ、処理可能なメディアの種類の数に制限がない方法が必要とされている。本発明は、この問題に対処し、前述の問題を解決しようとするものである。

【００１０】

【課題を解決するための手段】本発明の第１の態様によると、権利管理インターフェイスを電子メディア・コンテンツに保存し転送し及び/または提供するセキュア電子メディア・コンテナが提供される。このコンテナは、その中に格納される電子メディア・コンテンツと、コンテナの外部に付け足されるかまたは他の方法で関連付けられるデータと、典型的なメディア・ハンドラと、及び/またはコンテンツを開いて再生するために必要な権利管理メカニズムとを備えている。

【００１１】本発明の第２の態様によると、本発明の第１の態様によって定義されたセキュア・コンテナのコンテンツを処理する装置が提供され、このセキュア・コンテナには任意のフォーマットの電子メディア・コンテンツが格納される。この装置は、コンテンツのパッケージ化に使用された権利管理メカニズム（もしあれば）が何であるかを外部のデータから決定し、適切なデジタル権利管理ハンドラを取り出すかまたはそれにアクセスする手段と、ＤＲＭハンドラを介してコンテンツを渡す手段と、コンテンツへのアクセスと処理に必要なメディア・ハンドラを外部のデータから決定し、適切なメディア・ハンドラを取り出すかまたはそれにアクセスする手段と、メディア・ハンドラを介してコンテンツを渡す手段を備えている。

【００１２】さらに、本発明の第２の態様によると、本発明の第１の態様により定義されたセキュア・コンテナを処理する方法も提供され、このセキュア・コンテナには任意のフォーマットの電子メディア・コンテンツが格納される。この方法には、外部データを読み取ってコンテンツのパッケージ化に使用された権利管理メカニズム（もしあれば）が何であるかを決定し、適切なデジタル権利管理ハンドラを取り出すかまたはそれにアクセスするステップと、ＤＲＭハンドラを介してコンテンツを渡すステップと、外部データを読み取ってコンテンツへのアクセスと処理に必要なメディア・ハンドラを決定するステップと、適切なメディア・ハンドラを取り出すかまたはそれにアクセスするステップと、メディア・ハンドラを介してコンテンツを渡すステップが含まれる。

【００１３】セキュア・コンテナの概念は当分野において周知であり、本明細書ではデータを格納するための抽象的なデータ・コンテナ・フォーマットの観点から広く定義される。格納されたデータを包囲し保護する概念的なパッケージするなわち「ラッパ」を備えるコンテナの内部で、データは暗号化されるかまたは他の方法で調整されており、そのフォーマットのために特に調整された特定のソフトウェア・プログラムを使用した場合にのみ、データを再構築して使用できるようになっている。従来技術によるセキュア・コンテナの場合では、前述の特定ソフトウェア・プログラムによる以外は、コンテナの外部ではデータにもそれに関連する情報にもアクセスすることができず、再構築することもできない。

【００１４】一方、本発明は、任意のメディア・フォーマットと任意のＤＲＭメカニズムを考慮した普遍的な「エンベロープ」すなわちメタコンテナの形態でセキュア・コンテナを提供する。これは、メタデータをメディア・コンテンツを含むセキュア・コンテナに付け足すかまたは結びつけることによって実現される。一般に、メタデータは普遍的に読み出し及び/または解読が可能であり、コンテンツの「パッケージ化」に使用される根底の（underlying）メディア・フォーマットとデジタル権利管理メカニズムを記述するので、処理アプリケーション（例えば、デスクトップ・ソフトウェア・ツール、Ｗｅｂブラウザなど）は、コンテナの処理条件の評価、処理するコンポーネントの取り出し（必要であれば）、著作権者情報の取り出しと表示、及び指定された著作権管理ポリシーの適用が可能になる。

【００１５】メディア・コンテナの「外層」のフォーマット（パッケージまたは「ラッパ」それ自体とみなすことができる）は標準化することができ、このフォーマットは、様々なＤＲＭベンダーが異なる価値の提案に基づいて「プラグイン」解決法を作成することのできるメカニズムを提供するので、本発明の概念を使用して容易に相互運用性を実現することができる。これらのＤＲＭプラグインはそれぞれ必要に応じて独自のプロトコルを適用するように構成され、いかなるＤＲＭユーザー・インターフェイス、キー管理、トランザクション・メッセージング等が要求されてもそれを送り出すことができる。これらは、対象とするメディア表示アプリケーションに対する機能拡張として現れる。

【００１６】

【発明の実施の形態】図１を参照して、録音物等の電子コンテンツを含むセキュア・コンテナ１２をユーザー１０に送信する状況について考察する。データはセキュア・コンテナ１２に格納されているので、録音物を再構築し再生するには特別なソフトウェアが必要となる。一般的なコンテナ・ハンドラ１５は、セキュア・コンテナ１２内のデータをパッケージ化するために使用されたＤＲＭメカニズムの詳細（もしあれば）と、データを処理するために必要なメディア・ハンドラの詳細を取り出す。これらの詳細は、必要なメディア・ハンドラとＤＲＭハンドラを（それらがもし適当であれば）どのように（またはどこで）取得できるかについての詳細と共に、コンテナ１２の外層にメタデータとして付けられている。コンテンツはまず指定されたＤＲＭハンドラ１４を介して渡され、次に指定されたメディア・ハンドラを介して渡され、その結果、ユーザーは録音物を再生することができ、また適切なＤＲＭポリシーを適用することができる。

【００１７】（メタデータに含まれる）ＤＲＭフォーマットの規格は、一般的なコンテナ（またはエンベロープ）ハンドラ１５が必要とするメディア・ハンドラ１６を認識し参照し、及び/または（必要ならば）取り出す方法を表しており、特に、特定のＤＲＭハンドラまたはプラグインを認識し参照するための方法を表している。ＤＲＭメカニズムは、ＭＩＭＥタイプが現在処理されているのと同様の方法で参照することができる。

【００１８】コンテナ・ハンドラ及び/またはメディア・ハンドラがそれぞれのホスト・アプリケーションと通信する方法は様々なレベルで発生し、当分野において周知であるので、ここではこれ以上詳細には説明しない。ＤＲＭメカニズムが指定されているファイルをＤＲＭフォーマット・ハンドラが開くと、ＤＲＭフォーマット・ハンドラは、指定されたプラグインまたはリモート・サービスを呼び出してそれを処理する。しかし、このプラグインまたはサービスが行う内容、ユーザーとの通信方法及びネットワーク上での通信方法は本明細書とは関連せず、プログラムによって変わる。これによって、Ｗｏｒｄ、ＭＰ３、ＰＤＦ、ＨＴＭＬ等の任意のメディア・フォーマットを「マークアップ」として選択し、また任意のセキュリティ・ソリューションを用いてパッケージ化することができるという利点が得られる。換言すると、本発明はフォーマット・レベルのＤＲＭ相互運用性を提供すると見なすことができる。これによって、当事者が同一のメディア・フォーマットを使用しているように見えるが、実際には、本発明によって定義されたフォーマットのラッパ（ｗｒａｐｐｅｒ）を有するセキュア・コンテナを使用している。

【００１９】次に図２を参照して、本発明に従った例示的なマークアップ・フォーマットについて詳細に説明する。

【００２０】本発明の例示的な実施形態に従ったコンテナは、一般にＸＭＬなどの構造化マークアップ構文を使用しており、少なくとも＜ＣＯＮＴＥＮＴ＞セクションと＜ＤＲＭ＞セクションを備えている。

【００２１】＜ＣＯＮＴＥＮＴ＞セクションは、コンテンツのフォーマット（例えば、ＭＩＭＥタイプ）を指定する。このセクションは、コンテンツをカプセル化する（多くは１６進コードの「ブロップ（ｂｌｏｂ）」として）か、または、ネットワーク・リソースのアドレス（例えば、ＵＲＬまたはＤＯＩ）によって間接的に指定できるのが好ましい。＜ＣＯＮＴＥＮＴ＞セクション内の他の要素には、記述的メタデータ、フォーマット規格のＷｅｂロケーションへの参照（オプション）、「レンダリング」コード・レジストリのロケーションへの参照（オプション）が含まれる。

【００２２】＜ＤＲＭ＞セクションは、コンテンツのパッケージ化に使用するＤＲＭメカニズム（典型的にはメディア専用の暗号化メカニズム）を指定する。指定されたメカニズムは、＜ＣＯＮＴＥＮＴ＞セクションに含まれているか、または＜ＣＯＮＴＥＮＴ＞セクションで参照されている。ＤＲＭの参照先は、ローカル・システムにインストールされているコンポーネントか、遠隔のコンポーネントまたはウェブ・サービスである。従って、ＤＲＭフォーマットによって、ローカルの・コンテンツ・ブロップを遠隔のＤＲＭウェブ・サービスに処理のために送信するべきか、リモートの暗号化されたコンテンツ・ストリームをリモートのウェブ・サービスで解凍するべきか、または、リモート・ソース・ストリームをローカル・リソースで処理するべきかを指定することができる。

【００２３】＜ＤＲＭ＞コンテナ内の要素（ファイルまたはストリーム）の処理順序は、常に＜ＤＲＭ＞要素の後に＜＜ＣＯＮＴＥＮＴ＞要素が続く順序である。従って、呼び出しアプリケーションが外側のＤＲＭエンベロープを開き、ＤＲＭメカニズムが指定されていることを判定すると、このアプリケーションは、ＤＲＭフォーマットの所与の定義によって、まず指定されたＤＲＭメカニズム（フィルタのような）を経由してコンテンツを渡し、次に適切なメディア・ハンドラを呼び出してコンテンツ・タイプを処理しなければならないことを認識する。このような処理モデルによって、マルチステップＤＲＭメカニズムなどの高度なアプリケーションが可能になり、コンテンツは指定された一連のＤＲＭメカニズムによって渡される。

【００２４】オブジェクトのメディアタイプの適切な処理は、アプリケーションに依存することに注意する必要がある。例えば、埋め込まれた＜ＤＲＭ＞オブジェクトを使用してハンドラがＨＴＭＬファイルの「コード変換」を行う役割を持つ特定の場合において、正しい「処

理」方法は、コンテンツの指定されたＭＩＭＥタイプに合わせた適切なＨＴＭＬタグを出力ストリームに挿入することである。

【００２５】１つの考えられる実装では、ＤＲＭメカニズムは、それ自体の処理を経由してコンテンツから「抽出」したメタデータ構造（例えば、ＸＭＬファイル）を移管することができる。これは、メディア・ハンドラによって強化することができる（例えば、すでに埋め込まれている固有の権利メタデータによって）。それとは関係なく、プロキシ・サーバー装置（ａｐｐ）の呼び出しは、コンテンツを処理すべきであるとＤＲＭメカニズムが「述べる」やり方の（例えば）ＸＭＬでフォーマットされた規格を受け取る（どちらかといえば）。従って、ＤＲＭメカニズムは、メニュー項目等を制御する方法についてａｐｐに「提案」を渡すことができる。それを実際に行うのはａｐｐの役割である。複数のメカニズムを使用する場合には（「フィルタ」概念）、一組の規格が最終的にはａｐｐに渡されるように、制御メタデータがパッケージ化される。

【００２６】要約すると、本発明は電子データを保存及び/または転送する単一の「コンテナ」を提供する。このコンテナには、カプセル化されたデータのフォーマットを広範囲の様々なアプリケーションに対して指定し、データのパッケージ化に使用された権利管理技術を参照し、さらにデータ・コンテンツを取得し解釈する方法に関するポリシーを提供するために使用することのできるデータが（「コンテナ」の外部に）含まれる。

【００２７】本発明には例として以下の実施形態が含まれる。

【００２８】１．権利管理インターフェイスを電子メディア・コンテンツに保存し転送し及び/または提供するセキュア電子メディア・コンテナ（１２）であって、前記コンテナは、その中に格納される前記電子メディア・コンテンツと、該コンテナ（１２）の外部に付け足されるかまたは該コンテナに関連付けられるデータと、典型的なメディア・ハンドラ（１６）と、前記コンテンツを開いて再生するために必要な権利管理メカニズムとを備えるセキュア電子メディア・コンテナ。

【００２９】２．任意のフォーマットの電子メディア・コンテンツが格納される、上記１に記載のセキュア・コンテナ（１２）のコンテンツを処理する装置であって、もしあれば、前記コンテンツのパッケージ化に使用されたデジタル権利管理メカニズム（１４）が何であるかを前記外部のデータから決定し、適切なデジタル権利管理ハンドラ（１４）を取り出すかまたはそれにアクセスする（１５）手段と、前記デジタル権利管理ハンドラ（１４）を介して前記コンテンツを渡す手段と、コンテンツへのアクセスと処理に必要なメディア・ハンドラ（１６）を前記外部のデータから決定し、適切なメディア・ハンドラを取り出すかまたはそれにアクセスする手段と前記メディア・ハンドラ（１６）を介して前記コンテンツを渡す手段と、を備える装置。

【００３０】３．普遍的に読み出し及び/または解読が可能でありコンテンツのパッケージ化に使用された根底の（underlying）メディア・フォーマットとデジタル権利管理メカニズムを記述するメタデータが付属するまたは結合されているメディア・コンテンツを有するセキュア・コンテナを含む、上記１に記載のセキュア電子メディア・コンテナ（１２）。

【００３１】４．前記メタデータは、コンテンツ自体をカプセル化する根底のメディア・フォーマットを記述する、上記３に記載のセキュア電子メディア・コンテナ。

【００３２】５．前記メタデータは、コンテンツ自体が保存されているリモート・ネットワーク・リソース・アドレスを含む根底のメディア・フォーマットを記述する、上記３に記載のセキュア電子メディア・コンテナ。

【００３３】６．前記メタデータは、前記コンテンツ、フォーマット規格のリソース・ロケーションへの参照、「レンダリング」コード・レジストリのロケーションへの参照のいずれか１つ以上に関連する記述的メタデータを含む、上記３に記載のセキュア電子メディア・コンテナ。

【００３４】７．コンテンツのパッケージ化に使用されたデジタル権利管理メカニズムを記述する前記メタデータが、ローカル・システム上にインストールされたコンポーネント、リモート・コンポーネントまたはネットワーク・サービスを参照することができる、上記３に記載のセキュア電子メディア・コンテナ。

【００３５】８．任意のフォーマットの電子メディア・コンテンツが格納される上記１に記載のセキュア・コンテナ（１２）のコンテンツを処理する方法であって、前記外部のデータを読み取って、もしあれば前記コンテンツのパッケージ化に使用されたデジタル権利管理メカニズム（１４）が何であるかを決定し、適切なデジタル権利管理ハンドラ（１４）を取り出すかまたはそれにアクセスするステップと、前記デジタル権利管理ハンドラ（１４）を介して前記コンテンツを渡すステップと、前記外部のデータを読み取って、コンテンツへのアクセスと処理に必要なメディア・ハンドラ（１６）を決定するステップと、適切なメディア・ハンドラを取り出すかまたはそれにアクセスするステップと、前記メディア・ハンドラ（１６）を介して前記コンテンツを渡すステップと、を備える装置。

【００３６】以上のように、特定の例示的な実施形態を参照して本発明を説明した。しかし、本発明の精神と範囲を逸脱せずに様々な変形や変更が可能なことは当業者には明らかであろう。従って、本明細書及び図面は限定ではなく実例とみなされるべきである。

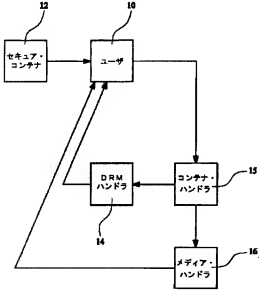
【図面の簡単な説明】

【図１】本発明の例示的な実施形態の機能を説明する概

略ブロック図である。
【図２】本発明に従った典型的なＤＲＭファイル・フォーマットを示す図である。
【符号の説明】

１２　電子メディア・コンテナ、セキュア・コンテナ
１４　権利管理メカニズム、ＤＲＭハンドラ
１５　コンテナ・ハンドラ
１６　メディア・ハンドラ

【図１】




【図２】

```
<?xml version="1.0" encoding="UTF-8"?>
<!--  これは、DRMフォーマットの一例のモックアップである  -->
<envelope>
    <content>
        <dc_elements>
            <!-- Dublin Core属性セットを用いた記述的メタデータ
            http://purl.org/DC/documents/ rec-dces-19990702.htm を参照のこと-->
                <title/>
            <creation/
            <subject/
            <description/
            <publisher/
            <contributor/
                <date/
                <type/
            <format value=" " version=" " specification=" " handler=" "/>
            <identifier/>
            <source/>
            <language/>
            <relation/>
            <coverage/>
            <rights/>
            </dc_elements>
        <content_location/>
        <content_blob/>
    </content>
    <drm>
        <drm_type value=" " version=" " specification=" " handler=" "/>
        <drm_blob/>
        <drm_location/>
    </drm>
</envelope>
```

フロントページの続き

(72)発明者 マーク・スカラジェーター
アメリカ合衆国03054ニューハンプシャー
州メリマック、スコッチ・パイン 14